(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 464 562 A3**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: **91110385.1**

(51) Int. Cl.5: **H04L 29/06**

(22) Date of filing: **24.06.91**

(30) Priority: **29.06.90 US 546628**

(43) Date of publication of application:
08.01.92 Bulletin 92/02

(84) Designated Contracting States:
DE FR GB IT NL

(88) Date of deferred publication of the search report:
04.11.92 Bulletin 92/45

(71) Applicant: **DIGITAL EQUIPMENT CORPORATION**
146 Main Street
Maynard, Massachusetts 01745(US)

(72) Inventor: **Hawe, William R.**
16 Independence Road
Pepperell, Massachusetts 01463(US)
Inventor: **Lampson, Butler W.**
180 Lakeview Avenue
Cambridge, Massachusetts 02138(US)
Inventor: **Gupta, Amar**
35 Woodstone Road
Northboro, Massachusetts 01532(US)

(74) Representative: **Betten & Resch**
Reichenbachstrasse 19
W-8000 München 5(DE)

(54) **Method and apparatus for decryption of an information packet having a format subject to modification.**

(57) A technique to facilitate decryption processing of information packets transmitted over a communication network after encryption in accordance with a specific network protocol, the details of which may be subject to later change as standards are developed or modified. Programmable registers are used in the decryption process to hold information for identifying an incoming information packet as being subject to the specific protocol and requiring decryption, and identifying a starting location of a data field to be decrypted. Specifically one programmable register contains a first offset locating an identifier field in the packet, in which a cryptographic identifier will be found if the packet is one conforming to the protocol; another programmable register contains a cryptographic identifier value that will be found in the identifier field if decryption is to be performed, and a third programmable register contains a second offset to locate the beginning of a data field to be decrypted.

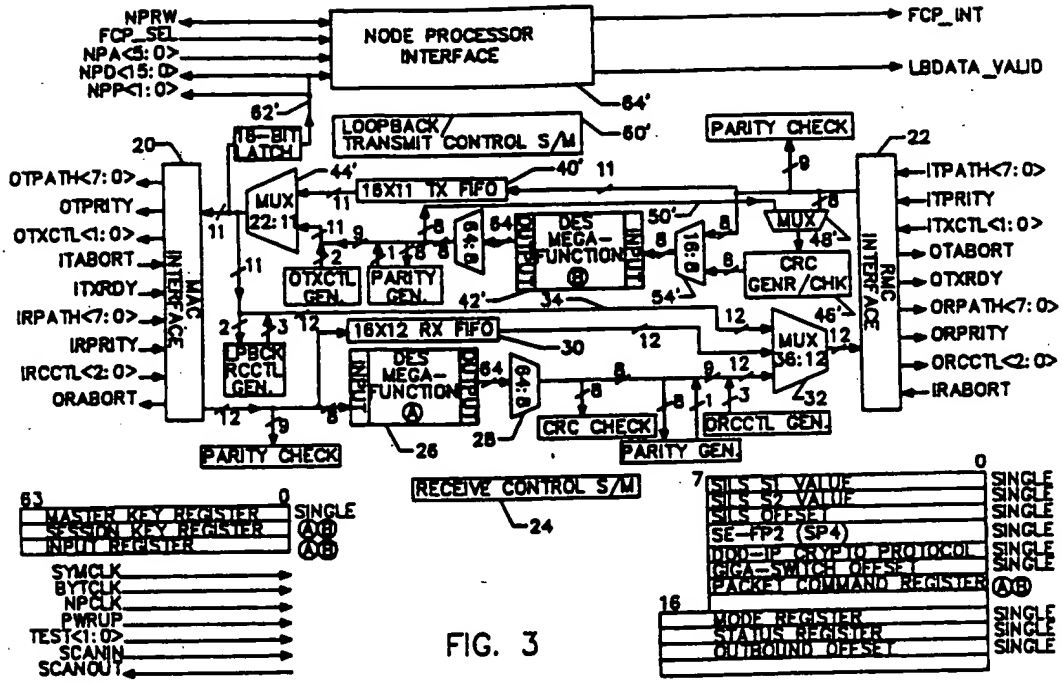
NPRW
FCP_SEL
NPA<5:0>
NPD<15:0>
NPP<1:0>
NODE PROCESSOR INTERFACE
FCP_INT
LBDATA_VALID
62'
16-BIT LATCH
LOOPBACK/ TRANSMIT CONTROL S/M
60'
64'
PARITY CHECK
22
20
OTPATH<7:0>
OTPRITY
OTXCTL<1:0>
ITABORT
ITXRDY
IRPATH<7:0>
IRPRITY
IRCCTL<2:0>
ORABORT
MAC INTERFACE
MUX 22:11
44'
40'
16X11 TX FIFO
ITPATH<7:0>
ITPRITY
ITXCTL<1:0>
OTABORT
OTXRDY
ORPATH<7:0>
ORPRITY
ORCCTL<2:0>
IRABORT
RNIC INTERFACE
OTXCTL GEN.
PARITY GEN.
64:8
DES MEGA-FUNCTION
8:16
MUX 48:8
CRC GENR/CHK
42'
34
50'
54'
46'
16X12 RX FIFO
30
MUX 36:12
LPBCK RCCTL GEN.
26
28
CRC CHECK
PARITY GEN.
ORCCTL GEN.
32
PARITY CHECK
RECEIVE CONTROL S/M
24
63
0
MASTER KEY REGISTER
SESSION KEY REGISTER
INPUT REGISTER
SINGLE
A/B
SYMCLK
BYTCLK
NPCLK
PWRUP
TEST<1:0>
SCANIN
SCANOUT
7
0
SILS S1 VALUE
SILS S2 VALUE
SILS OFFSET
SE-FP2 (SP4)
IDDO-IP CRYPTO PROTOCOL
GIGA-SWITCH OFFSET
PACKET COMMAND REGISTER
16
MODE REGISTER
STATUS REGISTER
OUTBOUND OFFSET

FIG. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 91 11 0385

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
Y	EP-A-0 289 248 (ATT) * page 2, line 52 - page 3, line 14 * * page 3, line 35 - line 54 * * page 4, line 44 - line 54 * * page 5, line 29 - line 43 * * figures 1-3 *	1,2,4	H04L29/06
Y	CCITT RECOMMENDATION X.509 vol. VIII, no. 8, 14 November 1988, MELBOURNE, AU 'DATA COMMUNICATION NETWORKS: THE DIRECTORY - AUTHENTICATION FRAMEWORK' * paragraph 1.6 * * paragraph 8.4 * * paragraph 8.5 *	1,2,4	
A	EP-A-0 279 232 (IBM) * column 7, line 21 - column 8, line 1 *	1-5	
A	GB-A-2 200 818 (INTEL) * page 1, line 1 - line LAST * * page 9, line 20 - line 23 * * claim 1; figure 1 *	1-5	TECHNICAL FIELDS SEARCHED (Int. Cl.5) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	04 SEPTEMBER 1992	CANOSA ARESTE C.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)